AFRL-IF-RS-TR-2006-350
In-House Interim Technical Report
December 2006

COALITION NETWORK MANAGEMENT SYSTEM

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the Air Force Research Laboratory Rome Research Site Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-IF-RS-TR-2006-350 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/

DAVID L. BIBIGHAUS, Major, USAF
Chief, Distributed Info Sys Branch
Advanced Computing Division

/s/

WARREN H. DEBANY, Jr.
Technical Advisor, Advanced Computing Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
DEC 2006	Interim	Sep 04 – Sep 06

4. TITLE AND SUBTITLE

COALITION NETWORK MANAGEMENT SYSTEM

5a. CONTRACT NUMBER In-House

5b. GRANT NUMBER N/A

5c. PROGRAM ELEMENT NUMBER 62702F

6. AUTHOR(S)

Eugene D. Turnbaugh

5d. PROJECT NUMBER 4519

5e. TASK NUMBER CN

5f. WORK UNIT NUMBER MS

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

AFRL/IFGA
525 Brooks Road
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/IFGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2006-350

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# 06-792

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Under the auspices of The Technical Cooperation Program, a Project Arrangement (PA) entitled Coalition Command Control and Communications Demonstration Environment (CC3DE) between the US, Australia and Canada was created and realized from 2000 to 2003. Those three nations collaborated on a Coalition Network Management System (CNMS) under the CC3DE PA. A new PA, entitled Policy Enabled Coalition Communications (PECC), will incorporate the United Kingdom and will iterate the design and concept of CNMS. As of this interim report, the PA still has not been signed due to export control language differences between nations. It is expected the PA will be signed by the end of 2006. Despite the limitation of an unsigned PA, AFRL has moved forward with in-house work on policy-based solutions for the coalition environment, to include: designing a modern service oriented architecture (SOA) for the coalition enterprise; identifying requirements for secure, cross-domain exchange of SOA protocols; begin design of reasoning resource monitors using semantic technology; and creating a NM protocol generator to test NM tool scalability.

15. SUBJECT TERMS

Coalition network management, network management, policy-based networking

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Eugene D. Turnbaugh
U	U	U	UL	15	19b. TELEPHONE NUMBER (*Include area code)*

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Table of Contents

Table of Figures

1.0 Introduction

Under the auspices of the Technical Cooperation Program, Command, Control, Communications and Information Systems Group, Technical Panel 8, a Project Arrangement (PA) titled Coalition Command Control and Communications Demonstration Environment (CC3DE) between the US, Australia and Canada was created and realized from 2000 to 2003. Those three nations collaborated on a Coalition Network Management System (CNMS) under the CC3DE PA. A new PA, entitled Policy Enabled Coalition Communications (PECC), will incorporate the United Kingdom and will iterate the design and concept of CNMS. As of the writing of this interim report, the PA still had not been signed due to export control language differences between nations. It is expected the PA will be signed by end of 2006.

This report describes in-house work performed by Air Force Research Lab (AFRL) to explore policy-based network management (NM) solutions within the coalition environment. Despite the limitation of an unsigned PA, AFRL has moved forward with several developments, to include: designing a more modern service oriented architecture (SOA) for policy-enabling the coalition enterprise environment; developing requirements for secure cross-domain exchange of SOA protocols to fit this new model; leveraging advances in semantic technology to begin design of reasoning NM resource monitors; and finally creating an NM protocol generator (using Internet Protocol version 6) to test the scalability of NM tools.

1.1 Objectives

The PECC effort will progress the state of the art in network resource management, especially for coalition operations. This effort will align national research and development agendas, and improve interoperability in multi-national coalition operations. The main objectives are:

1. Demonstrate how network and traffic management can be partially automated to reduce the number of people required whilst also improving responsiveness, effectiveness and resilience, especially in a mixed high and low bandwidth environment over multiple bearer types.
2. Demonstrate how coalition network and traffic management can be achieved within a security architecture that is representative of US-led coalition operations.
3. Demonstrate how a coalition commander can be given visibility and control of the coalition network, with an interface that is appropriate for a military officer with military concerns rather than a technical expert.

The main technical thrust is to investigate a scalable, distributed network management and control approach that would address policy-enabled networking, integration of dissimilar bearer services, and management & security across different coalition domains. The results of this investigation will provide input to the formulation of future coalition network architectures.

1.2 Scope

The PECC project will operate and demonstrate at the enterprise level, endeavoring to achieve network management across the coalition infrastructure, giving a coalition commander full visibility and control over their network.

Specific scopes as related to main objectives:

1. Policy-enabled Network Control: Integrate policy-enabled coalition network management environment; continue development of more robust policy resolution methods; increase policy granularity to be more tailored to individual threats
2. Integrating Dissimilar Bearer Services: Integrate dissimilar bearer services; develop/expand military quality of service (QoS) routing and cost functions; develop/expand bandwidth management functions
3. Management and Security across different security domains: Develop/expand capability to dynamically manage the security between different domains; research potential for dynamically created groups while maintaining security boundaries

1.3 Task Distribution

Contributions of concepts, capabilities, and/or components are below.

1. Australia will:
    a. Research results, experiments and/or demonstrations of key issues affecting different routing strategies as applied to deployed tactical networks incorporating bearer services of differing characteristics.
    b. Develop an extension of the Military Bandwidth Broker (M-BB) functionality to provide (as much as possible) seamless QoS to mission-critical services whose traffic flows need to be switched between bearers of different characteristics in a dynamic fashion.
    c. Develop and demonstrate, as a contribution to the joint effort, a capability allowing the top level communications command hierarchy to monitor the status of network resources and use a policy to dynamically reallocate the resources at a coarse level and in accordance with mission priorities.
2. Canada will:
    a. Investigate a capability that each bearer service component needs to allow QoS over that bearer service.
    b. Design components that optimize network and transport protocols to improve traffic performance over the various bearers being used.
    c. Develop a component that enables management and policy-control of QoS across an integrated infrastructure consisting of a variety of bearer services.
    d. Create a demonstrator application that manages all aspects of the QoS components.
3. UK will:

   a. Configure an (existing) UK test-bed to represent UK networks. This test-bed will also have IPv6 capabilities to emulate possible future transition of UK systems to IPv6. This test-bed is provided with means to interconnect with other-nations' test-beds via ISDN and Internet.
   b. Develop a Coalition Information Infrastructure Management System (CIIMS) to manage the above UK emulated networks and interact with other nations' management systems, both as a subordinate to a foreign coalition manager and as the coalition manager.
   c. Design a component of the CIIMS that manages and policy-controls QoS across several bearer services in national and coalition scenarios—and integrate this with the US C2RMS.
   d. Enhance the UK test-bed to provide a Computer Network Defence capability for the UK networks represented thereon.
   e. Integrate computer network defence management with Network Management in the UK CIIMS, and use it to support joint research on network defense through the use of policy-based techniques.
4. US will:
   a. Make use of an improved and enhanced guard, capable of securely operating on both sides of the nation/coalition domain boundary
   b. Design a service-oriented architecture framework in which to install each nation's components with a C2RMS integration module to manage policy control components.
   c. Design a component for deploying/querying policy and management information.
   d. Develop a means to dynamically form secure communities of interest within the coalition (i.e. dynamic group formation)
   e. In accordance with evolving DoD QoS standards, develop a component that manages access and QoS across heterogeneous bearers, to include constrained Line-of-Sight (LOS) and Extended LOS bearers.
   f. Develop an interface between mobile ad hoc tactical networks and fixed infrastructure.
5. Joint contributions will:
   a. If sensible and possible: update software/hardware to support a dual-stack environment that enables both Internet Protocol (IP) version 4 (IPv4) and IPv6; ensure capabilities are policy-enabled; follow best-practice methods, to include Internet Engineering Task Force (IETF) Request For Comment (RFC) standards (or equivalent).
   b. Continue development and expansion of policy-enabled networking, especially in connection with the rapid formation, optimization and defense of coalition networks. Joint demonstration of capability enhancement.
   c. Integrate dissimilar bearers within a coalition network scenario to enable performance optimization and provide resilience. Joint demonstration of capability enhancement.

d. Demonstrate capability-based scenarios that meet the demonstration needs of all the coalition partners.
e. Determine the procedures for developing, installing, using, and documenting the PECC environment software and hardware.
f. Demonstrate the concept of a high level capability, available to the top level communications command hierarchy, to assess multiple domain (national and coalition) network and information system status to assist mission planning. In addition, allows the changing of high level policies, reallocating resources at a coarse level, in accordance with mission priorities. This capability should enable interfacing with typical applications/tools resident within Network Operations Centers.
g. Enhance each nation's test-beds to include such security functionality (cryptography, firewalls, computer network defense, authentication, etc.) as would be appropriate at the interconnections between national systems in a coalition network. These functions may be emulated, or use lower-fidelity commercially or openly available substitutes for military-grade functions where necessary. In particular, for interconnection of Allies with the US, these functions need to be consistent with the Global Information Grid – Enterprise Services (GIG-ES) and GIG – Information Assurance (GIG-IA) architectures, which the US will verify.
h. Perform demonstration and/or integration of developed capabilities/components on the Combined Federated Battle Lab Network (CFBLNet) with interested nations.
i. Provide end of year-two joint analyses and report as well as joint final analyses and reports

1.4 Scheduling of Tasks

For period of activity, there will be three spirals, each 12 months in duration, and each including the following overlapping phases:

1. Analyze - Resolve objectives, discuss alternatives, and identify constraints/risks (first 4 months of spiral)
2. Evaluate - Evaluate design alternatives and their risks (months 2 - 5 of spiral)
3. Develop - Develop next evolutionary prototype (months 5 - 12 of spiral)
4. Review - Review outcome and plan next cycle (months 11 - 12 of spiral)

During spiral 1, projected to begin upon signing of PA:

- Jointly construct a fully integrated test bed by adding UK to the current US, Canada, and Australia integrated test beds. Following the joint engineering of the new system, if required, the UK will be provided any applicable disclosable information per the CC3DE PA.
- Jointly review the collaborative policy-based network pieces (i.e. software code and software architecture) for update and reengineering.
- Individual nations will define, categorize, and prioritize system components (corresponding to desired capabilities) for each nation's contributions

- Individual nations will define the means of communication between the components
- Individual nations will identify the core infrastructure needed to support the components.

During spiral 2,

- Jointly integrate policy-based networking software and demonstrate policy-based networking capability with all integrated components.
- Jointly demonstrate new capabilities on a frequent basis, if only to act as integration tests.
- Individual nations will ensure core (i.e. essential) and functional (i.e. used as building blocks) capabilities are implemented during this spiral, with some implementation of operational (i.e. exposed to other components) capabilities that demonstrate these new capabilities.

During spiral 3:

- Jointly participate in a full system demonstration using realistic scenarios showing how each nation's contribution meets the objectives and scope of this agreement.
- Jointly produce a joint technical paper for publication of the releasable, collaborative efforts over the project period.
- Individual nations will demonstrate their capabilities and concepts within different scenarios
- If resources permit, individual nations may add functionality by developing extension capabilities (i.e. optional, extra value capabilities), and demonstrate these with smaller, highly focused scenarios design to showcase the value added. The capabilities should approximate the full operational behavior and be capable of supporting the core demonstrations scenarios.

1.5 Demonstrations

The concept of policy-based networking using CNMS has been briefed and/or demonstrated over the last two years to:

- National Security Agency, in their role as the responsible party for the Global Information Grid (GIG) Information Assurance
- Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Summit
- Australian Defence Acquisition representatives
- AF Scientific Advisory Board
- UK distinguished visitors

In all cases, the concept was identified as an area in need of greater research due to its primary benefit of abstracting away technical details of written policies.

2.0 Summary of In-House Activities

2.1 Architecture

The original architecture of CNMS follows closely the architecture of DoD certified solutions (e.g. Combined ENTerprise Regional Information eXchange system (CENTRIX)). After semi-annual meetings with PECC participants over the last 2 years, it was decided that PECC will follow the same logical architecture with minimal changes (see Figure 1), while updating the implementation to include IPv6 and a more modern service oriented architecture. The AFRL original CNMS architecture's certification and accreditation (C&A) expired in September 2006 – it will need to be re-accomplished prior to live experimentation. The C&A documentation is well under development and should be ready for entry into the approval process by end of 2006.

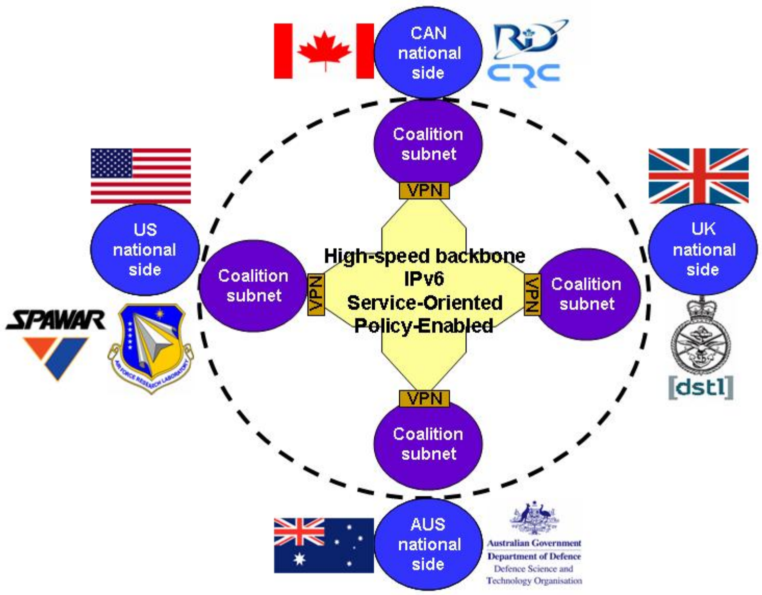

Figure 1 - PECC Basic Architecture

Whereas the original CNMS architecture relied on the Common Object Request Broker Architecture (CORBA) for the accessing of services offered by other nation's tools, the US has taken the lead in developing a new Service Oriented Architecture (SOA) based on eXtensible Markup Language (XML) using the eXtensible Messaging and Presence Protocol (XMPP). AFRL documented the 'pain threshold' of migrating the CNMS CORBA policy-based system to a PECC XMPP approach (see Figure 2) and presented this concept to coalition partners at meetings in both UK and Australia. PECC participants embraced the idea of moving from CORBA to XMPP.

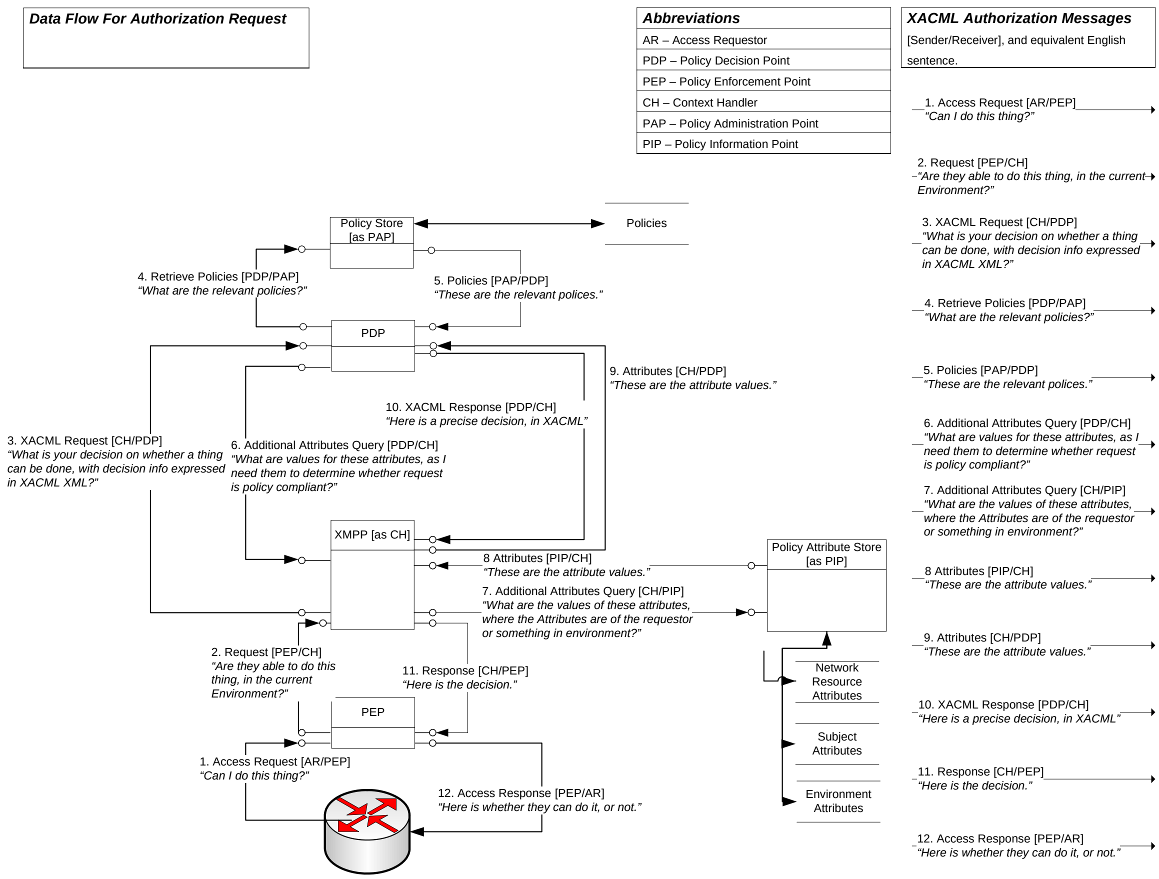

Figure 2 - SOA Implementation of Policy-based Networking

2.2 Cross-Domain Network Management using XMPP

As described in the introduction, the US continues its development of add-ons to accredited cross-domain guard technology, specifically the Information Support Service Environment (ISSE) Guard. With the move to a newer SOA, resource management (i.e. feedbacks from NM agents) may take the form of XMPP messages, which will now need to be handled in cross-domain flow of NM information. AFRL provided technical inputs to the Multi-Domain Resource Management System (MDRMS) project to incorporate XMPP threads into developmental versions of the ISSE Guard (see Figure 3). The guard only allows server to server communication. Both high-side and low-side XMPP servers are proxied by guard clients that are responsible for the following: session (state) management, security management, and transmission control protocol (TCP) connection monitoring. The guard thread provides schema based validation, security filtering and translation. Additionally, since IPv6 remains a focus of the PECC, the ISSE developers are updating the ISSE Guard to handle threads initiated in either IPv4 or IPv6, thereby meeting the DoD mandate for dual-stack support.

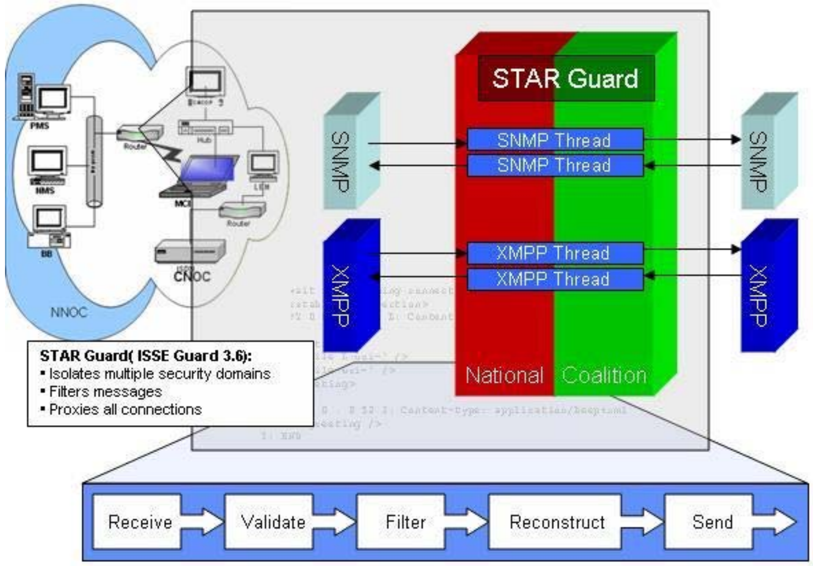

Figure 3 - Cross-domain Guard with XMPP Thread

AFRL is researching the both the utility of distributing low side proxies to each of the nations as well as the disclosure of an executable form of those low-side proxies for use in PECC architecture (see Figure 4).

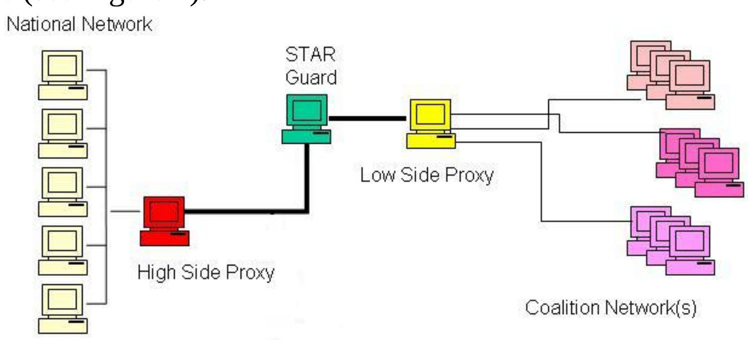

Figure 4 - Proposed Coalition Architecture with Guard

2.3 Resource Management

The adopted PECC architecture will allow for new mechanisms for resource management and development has begun on Service Augmented Resource Managers (SARM). The goal is to provide minimally intrusive resource management, using as few windows as possible. SARM will allow a focus on the tasks specific to each individual operator using one-glance awareness of task availability using caution panel style indicators. SARM will enable remote execution for simple resource operations (e.g. web server resource might have "stop" and "start") and optimally leverage semantic reasoning for resource monitoring -- truth table reasoning to deduce new Resource Description Framework (RDF) statements from an existing set of statements. This concept is similar to rule-based expert system, but with added flexibility. The primary GUI is an XMPP-capable chat program supporting relevant Jabber Enhancement Proposals (JEPs). There will be two tiers of agents: Tier 1 Monitors that access resource data (process creation, CPU load, disk space) and publish it in RDF via XMPP; Tier 2 Reasoners aggregate one or more published sets of RDF statements and publish derived RDF statements. Reasoners represent resources with availability, and their XMPP presence status reflects the resource's availability. XMPP client talks to Reasoners and sees resource availability within an Instant Messenger roster. Resources are grouped into task folders in the roster, which represent those resources necessary for completion of the task. Work continues on SARM. It will also be integrated as a resource management extension to C2RMS.

2.4 Network Management Logic System (NMLS)

When this in-house work began, the commercial industry lacked IPv6 compatible tools, which was understandable given the lack of US national interest in the protocol. After an examination of available tools, we found no product capable of spoofing IPv6 NM protocols, so we began in-house development of an IPv4/IPv6 NM protocol generator called NMLS. It's envisioned that as the number of manageable devices rises (due to roll-out of IPv6) that there may be a corresponding increase in the number of devices wishing to be managed – NMLS was built to help test the scalability of IPv6-comptabile NM tools. NMLS runs from a single laptop and is capable of spoofing thousands of "clients" using Internet Control Message Protocol (ICMP), ICMPv6, Address Resolution Protocol, Network Discovery Protocol, and specific Simple Network Management Protocol (SNMP) queries [specifically SNMPGet and GetNext] over IPv4/IPv6. All the "clients" appear as single, individually addressed machines, as shown in Figure 5.

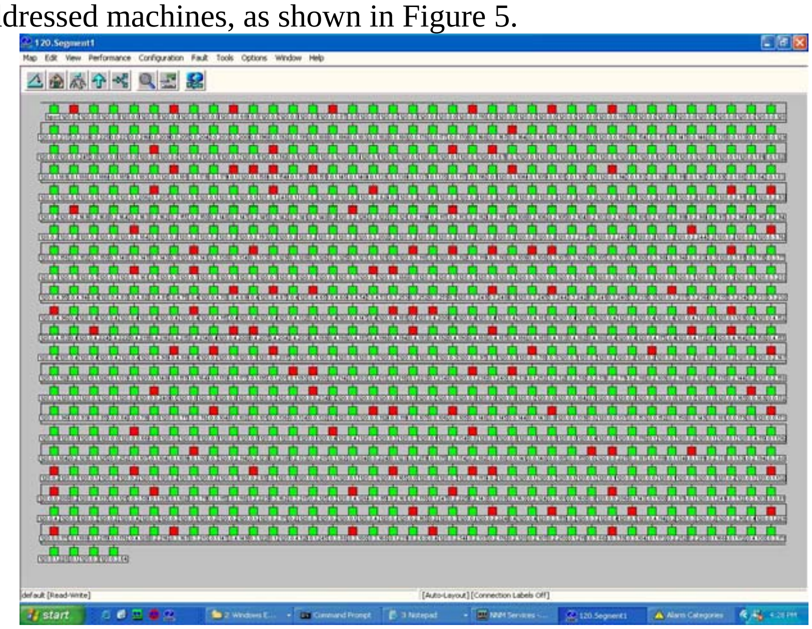

Figure 5 - NMLS 1000-node Screenshot

Recently, commercial products have become available that can spoof either IPv4 or IPv6 using numerous protocols (e.g. HTTP, SNMP, FTP, etc.) and are cheaper to use than the cost to continuing development on NMLS. NMLS remains available for use, but its development has been discontinued.

3.0 Continuing Developments

The PECC PA should be signed by the end of 2006. Once the PA is signed, an official technical kick-off will happen with each nation's technical staff. The program leads of each of the nation's have agreed to begin initial architecture work (i.e. getting the labs connected), which is covered under disclosure agreements already in place under TP8.

Development continues on SARM and MDRMS, as well as refining the architecture based on updated national projects. The UK has great interest in integrating their proposed CIIMS project with C2RMS as a test-case for cross-domain exchange of network management information. It's likely that GIG Network Centric Implementation Documents (NCIDs) will assist in building the requirements for the data exchange between systems. Canada has provided a prototype policy-based security manager for open use (as perhaps a baseline for the collaborative policy-based portion of PECC) among nations. It has policy enforcement points built for Fortigate devices (a router/firewall device). Australia is looking to continue policy-based network management research, and will also incorporate multi-topology routing (MTR). The US Navy's Space and Naval Warfare Systems Command (SPAWAR) continues to evolve its MTR and is researching how to bring their extensive Naval modeling lab to PECC.